5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

Enrollment x Design, LLC ("ExD") Incident Response Policy and Procedure

Incident Response Policy

1. DOCUMENT PURPOSE

1.1. This document defines the policy for addressing Security Incidents through appropriate Incident Response.

1.2. This document applies to all Personnel and supersedes all other policies relating to the matters set forth herein.

2. POLICY - TERMS & DEFINITIONS

Term/Acronym	Definition
Data Breach	A Security Incident that directly impacts Personal Data, Sensitive Personal Information or Personally Identifiable Information.
Data Controller	Means the person or organization that determines the purpose and means of the Processing of Personal Data.
Escalation	The engagement of additional resources to resolve a Security Incident.
Incident Response / Incident Management	Process for detecting, reporting, assessing, responding to, dealing with, and learning from Security Incidents.
Information Security	Preservation of confidentiality, integrity, and availability of Information and the equipment, devices or services containing or providing such Information.

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

Personal Data	Means any information relating to an identified or identifiable Data Subject, where such information is protected under applicable law. For clarity, Personal Data includes any SPD, SPI, and/or Tracking Data that directly or indirectly identifies a Data Subject.
Personnel	ExD employees (part and full time) and interns.
Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy, a possible exploitation of a Security Vulnerability or Security Weakness or a previously unknown situation that can be security relevant.
Security Incident	A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.
Security Incident Response Process (SIRP)	A process constituted for responding to a Security Incident, managed by the Information Security Department. During a Security Incident, the SIRP is responsible for communication with and coordination of other internal and external groups and securing appropriate external expertise as needed (e.g., technology, legal, communication, etc.)
Security Vulnerability	A weakness of an existing asset or control that can be exploited by one or more threats.
Security Weakness	A weakness that results from the lack of an existing, necessary control.

3. SCOPE

The objective of this policy is to ensure a consistent and effective approach to the management of Security Incidents, including the identification and communication of Security Events and Security Weaknesses.

4. INCIDENT RESPONSE POLICY

The Incident Response policy is as follows:

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to Security Incidents.
- The objectives for Security Incident management is to ensure and clarify the organization’s priorities for handling Security Incidents.

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

- Security Events should be reported through appropriate channels as quickly as possible
- Personnel and contractors using the organization's information systems and services are required to note and report any observed or suspected Security Weakness in systems or services
- Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.
- Security Incidents should be responded to in accordance with documented Incident Response procedures.
- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.
- Awareness should be provided on topics such as:
    - The benefits of a formal, consistent approach to Incident Management (personal and organizational);
    - How the program works, expectations;
    - How to report Security Incidents, who to contact;
    - Constraints imposed by non-disclosure agreements.
- Communication channels should be established well in advance of a Security Incident. Include all necessary parties in relevant communication:
    - SIRP participants
    - ExD Management
    - ExD Personnel or contractors
- In the event a Security Incident, Data Controllers, government bodies and other necessary parties should be notified in a reasonable timeframe, and in compliance with regulatory and other applicable requirements and guidance.
- **External security incident expertise may need to be secured if the internal capacity of the organization is unable to clarify and move forward an appropriate plan of action.**

INCIDENT RESPONSE PROCEDURES
5. DOCUMENT PURPOSE

1.3. The purpose of this document is to define the Incident Response procedures followed by ExD in the event of a Security Incident. This document is a step-by-step guide of the measures

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

Personnel are required to take to manage the lifecycle of Security Incidents within ExD, from initial Security Incident recognition to restoring normal operations. This process will ensure that all such Security Incidents are detected, analyzed, contained and eradicated, that measures are taken to prevent any further Security Incidents, and, where necessary or appropriate, that notice is provided to law enforcement authorities, Personnel, and/or affected parties

1.4. This document applies to all Personnel and supersedes all other procedures, practices, and guidelines relating to the matters set forth herein.

6. INCIDENT RESPONSE PROCEDURES - TERMS & DEFINITIONS

Term/Acronym	Definition
Abnormal Activities	Unsuccessful attacks that appear particularly significant based on ExD understanding of the risks it faces.
Data Breach	A Security Incident that directly impacts Personal Data, Sensitive Personal Information or Personally Identifiable Information.
Data Controller	Means the person or organization that determines the purpose and means of the Processing of Personal Data.
Escalation	The engagement of additional resources to resolve or provide the status regarding a Security Incident.
External Legal	External legal resources secured to provide advice and review during process.
Incident Record	Created at the time a Security Incident is initially recognized. Contains all relevant information pertaining to the Security Incident.
Incident Response / Incident Management	Process for detecting, reporting, assessing, responding to, dealing with, and learning from Security Incidents.

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

Information Security	Preservation of confidentiality, integrity, and availability of Information and the equipment, devices or services containing or providing such Information.
Personal Data	Means any information relating to an identified or identifiable Data Subject, where such information is protected under applicable law. For clarity, Personal Data includes any SPD, SPI, and/or Tracking Data that directly or indirectly identifies a Data Subject.
Personally Identifiable Information (PII)	Means any information about a Data Subject, whether in paper, electronic, or other form, which can be used to distinguish or trace an individual's identity, such as name, email address, or telephone number.
Personnel	ExD employees (part and full time) and interns.
Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy, a possible exploitation of a Security Vulnerability or Security Weakness or a previously unknown situation that can be security relevant.
Security Incident	A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.
Security Incident Response Process (SIRP)	A process constituted for responding to a Security Incident, managed by the Information Security Department. During a Security Incident, the SIRP is responsible for communication with and coordination of other internal and external groups and securing appropriate external expertise as needed (e.g., technology, legal, communication, etc.)
Sensitive Personal Information (SPI)	Means specific standalone PII or a combination of information that could identify, trace, or locate a Data subject, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
Security Vulnerability	A weakness of an existing asset or control that can be exploited by one or more threats.
Security Weakness	A weakness that results from the lack of an existing, necessary control.

7. SCOPE

This document covers the Incident Response process for all identified Security Incidents.

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

The following activities will be covered:

- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activities

The Incident Response process is considered complete once Information confidentiality, integrity, and/or availability are restored to normal and verification has occurred.

8. OVERVIEW

8.1. Roles and Responsibilities

Individuals needed and responsible for responding to a Security Incident include the following:

- ExD Management
- Outside legal providers
- Contractors (as necessary)
- Data managements
- Clients
- Communications Resources

9. PROCESS

9.1. Detection Phase

In the detection phase the SIRP, or an internal or external entity, identifies a Security Event that may be the result of a potential exploitation of a Security Vulnerability or a Security Weakness, or that may be the result of an innocent error.

Immediately upon observation or notice of any suspected Security Event, Personnel shall use reasonable efforts to promptly report such knowledge and/or suspicion to the Information Security Department at the following address:

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

- Email: InformationSecurity@ExD.com

A Security Event may be discovered in many ways, including the following:

- Observation of suspicious behavior or unusual occurrences;
- Lapses in physical or procedural security;
- Information coming into the possession of unauthorized Personnel or Third Parties.
- Information inappropriately exposed on a publicly facing website.

To assess whether a Security Event must be reported, Personnel should consider whether there are indications that:

- Information was used by unauthorized Personnel or Third Parties;
- Information has been downloaded or copied inappropriately from an ExD computer systems or equipment;
- Equipment or devices containing Information have been lost or stolen;
- Equipment or devices containing Information have been subject to unauthorized activity (e.g., hacking, malware).
- Personal Data has been publicly exposed.

In addition, the following situations should be considered for Security Event reporting:

- Ineffective security controls;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors (innocent or otherwise);
- Non–compliance with policies or standards;
- Breaches of physical security arrangements;
- Uncontrolled systems changes;
- Malfunctions of software or hardware;
- Access violations.

Even if it is not clear whether a Security Event is an actual Security Incident it is still incumbent to be cautious than to be compromised and follow procedures detailed below.

The SIRP will usually require the reporter to supply further information, which will depend upon the nature of the Security Event. However, the following information normally shall be supplied:

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

- Contact name and information of person reporting the Security Event;
- Date and time the Security Event occurred or was noticed;
- Type and circumstances of the Security Event;
- The type of data, information, or equipment involved;
- Location of the Security Event and data or equipment affected;
- Whether the Security Event puts any person or other data at risk; and
- Any associated ticket numbers, emails or log entries associated with the Security Event.

SIRP Primary Lead will ensure that the SIRP is promptly engaged once such notice is received. The following actions will also be taken:

1. The SIRP shall use reasonable efforts to analyze the matter within four (4) hours of notice and decide whether to proceed with the Analysis Phase of the Incident Response Procedures.

a. Determination to initiate the Analysis Phase must be made quickly so that Personnel can make an initial determination as to the urgency and seriousness of the situation.

2. Upon making the decision to begin the Analysis Phase, if the SIRP suspects that the Security Event may result in damage to the reputation of ExD or legal liability, the SIRP shall initiate a legal assessment of actual or potential legal issues.

9.2. Analysis Phase

The initial response to detection of a Security Event is typically the Analysis Phase. In this phase the SIRP determines whether or not a Security Event is an actual Security Incident. To determine if a Security Event is a Security Incident the following considerations apply:

1. Leverage diagnostic data to analyze the Security Event using tools directly on the operating system or application. This may include, but not be limited to:

(i) Taking screenshots, memory dumps, consult logs and network traces;

(ii) Performing analysis on the information being collected;

(iii) Analyzing the precursors and indications;

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

(iv) Looking for correlating information; and

(v) Performing research (e.g., search engines, knowledgebase).

2. Identify whether the Security Event was the result of an innocent error, or the actions of a potential attacker. If the latter, effort shall be made to identify who the potential attacker may be, by:

(i) Validating the attacker's IP address;

(ii) Researching the attacker through search engines;

(iii) Using incident databases;

(iv) Monitoring attacker communication channels, if possible; and

(v) In unique cases, and with the approval of legal counsel, potentially scanning the attacker's system.

If the SIRP has determined that a Security Event has triggered a Security Incident, the appropriate SIRP Process members will be engaged accordingly and the SIRP will begin documenting the investigation and gathering evidence. The type of Security Incident is based on the nature of the event. Example types are listed as follows:

1. Data exposure.

2. Unauthorized access.

3. Distributed Denial of Service/ Denial of Service (DDoS/DoS).

4. Malicious code.

5. Improper usage.

6. Scans/Probes/Attempted access.

If it is determined that a Security Incident has not been triggered, additional activities noted under '5.6. Post-Incident Activities' may be initiated under the direction of the SIRP.

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

The Security Incident's potential impact on ExD and/or its clients, partners, associates, constractors shall be evaluated and the SIRP shall assign an initial severity classification of low, medium, high or critical to the Security Incident. To analyze the situation, scope, and impact, the SIRP shall:

1. Define and confirm the severity level and potential impact of the Security Incident.

2. Identify which resources have been affected and forecast which resources will be affected.

3. Estimate the current and potential effect of the Security Incident.

The SIRP shall attempt to determine the scope of the Security Incident and verify if the Security Incident is still ongoing. Scoping the Security Incident may include collecting forensic data from suspect systems or gathering evidence that will support the investigation. It may also include identifying any potential data theft or destruction. New investigative leads may be generated as the collected data is analyzed. If the Security Incident involves malware, the SIRP shall analyze the malware to determine its capabilities and potential impact to the environment. Based on the evidence reviewed, the SIRP will determine if the Security Incident requires reclassification as to its severity or cause (e.g., whether it was originally thought to be the action of a malicious actor but turned out to be an innocent error, or vice versa).

As indicated above, a Security Incident may require evidence to be collected. The collection of such evidence shall be done with due diligence and the following procedures shall apply:

1. Gathering and handling of evidence (forensics) should include:

(i) ¬Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer);

(ii) Name, title, and phone number of everyone who collected or handled the evidence during the investigation;

(iii) ¬Time and date (including time zone) of each occurrence of evidence handling;

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

(iv) ¬Locations where the evidence was stored, and conditions of storage (e.g., locked spaces, surveilled spaces); and

(v) Reasonable efforts to create two backups of the affected system(s) using new, unused media — one is to be sealed as evidence and one is to be used as a source of additional backups.

2. To ensure that evidence is not destroyed or removed, where any associates, partners, or contractors are suspected of being responsible for a Security Incident, ExD shall, consistent with its procedures, use reasonable efforts to place monitoring and forensics agents and/or confiscate all computer/electronic assets that have been assigned to him or her.

(i) This task may be done surreptitiously, and should be completed as quickly and in as non-intrusive a manner as possible.

(ii) The SIRP should consider restricting access to the computers and attached peripherals (including remote access via modem, secure remote system access, etc.) pending the outcome of its examination.

3. Where applicable, and depending upon the seriousness of the Security Incident, items and areas that should be secured and preserved in an “as was” condition include:

(i) Work areas (including wastebaskets);

(ii) Computer hardware (keyboard, mouse, monitor, CPU, etc.);

(iii) Software;

(iv) Storage media (disks, tapes, removable disk drives, CD ROMs, etc.);

(v) Documentation (manuals, printouts, notebooks, notepads);

(vi) Additional components as deemed relevant (printer, cables, etc.);

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

(vii) In cases of damage, the computer system and its surrounding area, as well as other data storage devices, should be preserved for the potential collection of evidence (e.g., fingerprinting);

(viii) If the computer is "Off", it should not be turned "On". For a stand-alone computer system, if the computer is "On", the Information Security and IT Departments are to be contacted.

4. It is important to establish who was using the computer system at the time of the Security Incident and/or who was in the immediate area. The SIRP should obtain copies of applicable records as part of the investigation.

5. Based on the severity level and the categorization of the Security Incident, the proper Process or Personnel shall be notified and contacted by the SIRP.

6. Until the SIRP, with the approval of ExD management, makes the Security Incident known to other Personnel, the foregoing activities shall be kept confidential to the extent possible.

If it is determined that a Security Incident has occurred and may have a significant impact on ExD or its subscribers, the SIRP shall determine whether additional resources are required to investigate and respond to the Security Incident. The extent of the additional resources will vary depending on the nature and significance of the Security Incident.

Abnormal Activities Notification:

The SIRP recognizes that there may be many attempts to gain unauthorized access to, disrupt or misuse information systems and the information stored on them, and that many of these attempts will be thwarted by ExD' information security program. In general, the SIRP will not report unsuccessful attacks to customers. For example, the SIRP would generally not be required to report to a Data Controller or customer if it makes a good faith judgment that the unsuccessful attack was of a routine nature.

However, the SIRP will take reasonable steps to notify customers or Data Controllers of any identified Abnormal Activities. For example, in making a judgment as to whether a particular unsuccessful attack should be reported, ExD might consider whether handling the attack required

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

measures or resources well beyond those ordinarily used, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps. In cases of identified Abnormal Activities, the Data Controller or customer would be notified by means agreed upon by ExD and the Data Controller or customer within twenty-four (24) hours upon ExD becoming aware of the Abnormal Activity.

Data Breach Notification:

If it is determined during the analysis phase that a Security Incident has occurred that constitutes a Data Breach, with notification obligations based on regulatory, legal, or similar requirements, notification of such Data Breach shall be provided to the impacted Data Controller (client, stakeholder, partner) by email, telephone, or other means as necessary, within twenty-four (24) hours upon ExD becoming aware of the Data Breach. Additional activities noted under '5.6. Post-Incident Activities' may also be initiated under the direction of the SIRP.

9.3. Containment Phase

The Containment Phase mitigates the root cause of the Security Incident to prevent further damage or exposure. This phase attempts to limit the impact of a Security Incident prior to an eradication and recovery event. During this phase, the SIRP may implement controls, as necessary, to limit the damage from a Security Incident. If a Security Incident is determined to be caused by innocent error, the eradication phase may not be needed. For example, after reviewing any information that has been collected investigating the Security Incident the SIRP may:

1. Secure the physical and network perimeter.

    i. For example, shutting down a system, disconnecting it from the network, and/or disabling certain functions or services.

2. Connect through a trusted connection and retrieve any volatile data from the affected system.

3. Determine the relative integrity and the appropriateness of backing the system up.

4. If appropriate, back up the impacted system.

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

5. Change the password(s) to the affected system(s). Stakeholders and/or partners, as appropriate, shall be notified of the password change.

6. Determine whether it is safe to continue operations with the affected system(s).

i. If it is safe, allow the system to continue to function, in which case the SIRP will:

a. Update the Incident Record accordingly; and

b. Move to the Recovery Phase.

ii. If it is not safe to allow the system to continue operations, the SIRP will discontinue the system(s) operation and move to Eradication Phase.

iii. The SIRP may permit continued operation of the system under close supervision and monitoring if:

1. Such activity will assist in identifying individuals responsible for the Security Incident;

2. The system can run normally without risk of disruption, compromise of data, or serious damage; and

3. Consensus has been reached within the SIRP before taking the supervision and monitoring approach.

7. The final status of this stage should be appropriately documented in the Incident Record.

During the Analysis and Containment Phases, the SIRP shall keep notes and use appropriate chain of custody procedures to ensure that the evidence gathered during the Security Incident can be used successfully during prosecution, if appropriate.

9.4. Eradication Phase

The Eradication Phase is the phase where vulnerabilities causing the Security Incident, and any associated compromises, are removed from the environment. An effective eradication for a targeted attack removes the attacker’s access to the environment all at once, during a coordinated

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

containment and eradication event. Although the specific actions taken during the Eradication Phase can vary depending on the Security Incident, the standard process for the Eradication Phase shall be as follows:

1. Determine the symptoms and cause related to the affected system(s).

2. Eliminate components of the Security Incident. This may include deleting malware, disabling breached user accounts, etc.

3. Strengthen the controls surrounding the affected system(s), where possible (a risk assessment will be performed, if needed). This may include the following:

i. Strengthening network perimeter defenses.

ii. Improving monitoring capabilities or scope.

iii. Remediating any security issues within the affected system(s), such as removing unused services or implementing general host hardening techniques.

iv. Conduct a vulnerability assessment to verify that all the holes/gaps that can be exploited have been addressed

1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
2. Update the Incident Record with the information learned from the vulnerability assessment, including the cause, symptoms, and method used to fix the problem with the affected system(s).
3. Apprise management of progress, as necessary.

After ExD has implemented the changes for eradication, it is important to verify that cause of and individual(s) causing the Security Incident is fully eradicated from the environment. The SIRP shall also test the effectiveness of any security controls or changes that were made to the environment during containment and eradication.

9.5. Recovery Phase

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

The Recovery Phase represents the SIRP's effort to restore the affected system(s) to operation after the problems that gave rise to the Security Incident, and the consequences of the Security Incident, have been corrected.

Although the specific actions taken during the Recovery Phase can vary depending on the identified Security Incident, the standard process to accomplish this shall be as follows:

1. Execution of the following actions, as appropriate:

- Rebuilding systems.
- Changing passwords.
- Restoring systems from clean backups.
- Replacing affected files with clean versions.

2. Determination whether the affected system(s) has been changed in any way.

a. If the system(s) has been changed, the system is restored to its proper, intended functioning ("last known good").

i. Once restored, the system functions are validated to verify that the system/process functions as intended. This may require the involvement of the individual (or unit) that owns the affected system(s).

ii. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline), it should be restored and validated, and the system(s) should be monitored for proper behavior.

b. If the system(s) has not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.

1. Implementation of additional monitoring and alerting may be done to identify similar activities.
2. Update the Incident Record with any details determined to be relevant during this phase.
3. Apprise management of progress, as appropriate.
4. Post-Incident Activities

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

In addition to the Data Breach and Abnormal Activities notification requirements identified in the analysis phase above, and after verification of a successful containment and any necessary eradication, the SIRP shall take the following post-incident activities, as may be necessary:

I. Communications

A. Notification

When warranted or required by judicial action, law, or regulation, ExD shall use reasonable efforts to provide notice to Personnel and/or affected parties about a Security Incident involving the Sensitive and/or Confidential Information of such stakeholders. For example:

1. Where it has been determined, or the SIRP and management reasonably believe, that there has been unauthorized access to or release of unencrypted customer data;

2. Where the Security Incident has compromised the security, confidentiality or integrity of Confidential Information.

Upon deciding to notify the ExD shall use reasonable efforts to provide notice and disclosure to Personnel and/or affected parties within twenty-four (24) hours and, subject to applicable law, prior to notification of law enforcement personnel. Delay may nonetheless occur in instances where it is mandated or authorized by applicable law. For example, disclosure might be delayed if notice would impede a criminal investigation or if time is required to restore reasonable integrity to ExD's information systems.

If appropriate, the SIRP may:

1. Prepare a general notice and arrange for providing the notice to affected parties;

2. Prepare a FAQ based on the notice and arrange to have it posted to the ExD website after the notice has been sent;

3. Identify a point a contact for Personnel and/or affected parties to contact if further information is sought; and

4. Establish a toll-free number for use by stakeholders.

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

ExD's objective is to provide notice in a manner designed to ensure that Personnel and/or affected parties can reasonably be expected to receive the disclosure.

The form and content of the of notification may either be by letter (first class mail) or by email sent to an address where Personnel and/or affected parties can reasonably be expected to receive the disclosure or other, similar means.

The notification, in clear and plain language, may contain the following elements:

1. A description of the Security Incident that includes as much detail as is appropriate under the circumstances;

2. The type of information subject to unauthorized access;

3. Measures taken by ExD to protect the Information of Personnel and/or affected parties from further unauthorized access;

4. A contact name and toll-free number that Personnel and/or affected parties may use to obtain further information;

5. A reference to the page on the ExD website where updates may be obtained;

6. A reminder to guard against possible identify theft by being vigilant with respect to banking or credit activity for twelve to twenty-four months;

7. Contact information for national credit reporting agencies;

8. Other elements as may be required by applicable law or whose inclusion the SIRP may otherwise consider appropriate under the circumstances.

B. Cooperation with External Investigators

In the event that the management considers it appropriate to inform law enforcement authorities or to retain forensic investigators or other external advisors, the following information shall be collected to provide to such authorities or investigators:

1. To the extent known, details of the:

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

a. Security Incident (date, time, place, duration, etc.);

b. Person(s) under suspicion if know (name, date of birth, address, occupation/position, employment contracts, etc.);

c. Computer files pertaining to the Security Incident(s);

d. Details of any Information that is allegedly stolen, altered, or destroyed;

e. The access rights to the computer system involved as part of the investigation;

f. Any action taken in relation to the computer systems concerned, including the date and time.

2. A copy of applicable ExD Data Privacy and Security Policy ("Policy") in force at the time of the incident (if applicable); and

3. Any other documentation or evidence relevant to the internal investigation of the Security Incident.

C. Information Sharing and Media Relations

Security Incident-specific information (e.g., dates, accounts, programs, systems) must not be provided to any unknown individuals making such requests by telephone or email. Any release of Security Incident-specific information should only be to individuals previously identified by the SIRP. All requests for information from unknown individuals should be forwarded to the management. If there is any doubt about whether information can be released, contact the management.

Contact with law enforcement authorities shall only be made by the management.

The management, shall determine whether it is appropriate to issue a media statement, hold a press briefing, or schedule interviews.

If Sensitive and/or Confidential Information has been compromised and a significant number of individuals, as identified by the SIRP, are affected and/or suspected of being affected, the management, upon consultation with outside counsel and subject to applicable law, shall use

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

reasonable efforts to contact applicable consumer reporting agencies prior to sending notices to the affected parties.

Certain jurisdictions where ExD does business, or where ExD's stakeholders reside, mandate different disclosure or notification obligations. Additionally, advice from both inside and outside counsel is required before communication occurs with credit reporting agencies.

D. External Incident Communications

After a Security Incident, information may be required to be shared with outside parties, following emergency response procedures as necessary, including:

- Law enforcement/incident reporting organizations
- Affected external parties
- The media
- Other outside parties

1. ExD will seek to ensure its obligations are fulfilled by quickly and professionally taking control of communication early during major events. Accordingly, the SIRP will:

- Designate a credible, trained, informed spokesperson to address the media;
- Determine appropriate clearance and approval processes for the media;
- Ensure the organization is accessible by media so they do not resort to other (less credible) sources for information;
- Emphasize steps being taken to address the Security Incident;
- Tell the story quickly, openly, and honestly to counter falsehoods, rumors, or undue suspicion.

2. When publicly disclosing information of a Security Incident, the following should be considered:

- Was Personal Information compromised?
- Was subscriber data compromised?
- Were legal and/or contractual obligations invoked by the Security Incident?
- What is the organization's strategy moving forward?

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

E. Internal Incident Communications

1. Where warranted, the SI process will ensure that open communication is maintained within the organization to ensure relevant parties are informed of facts, reminded of responsibilities, and capable of dismissing rumors and speculation.

2. Aggregate documentation from post-mortem/follow-up reviews into the Security Incident record and create a formal report of the Security Incident to share with management, as necessary.

II. Follow Up

The Follow-up Phase represents the review of the Security Incident to look for "lessons learned" and to determine whether the process that was followed could have been improved in any way. Security Events and Security Incidents should be reviewed after identification resolution to determine where response could be improved.

The Security Event or Security Incident process creates, as necessary, and performs the following:

i) Determine the root cause of the Security Incident and what should be done to ensure that the root cause has been addressed

ii) Create a "lessons learned" document and include it with the Incident Record.

iii) Evaluate the cost and impact of the Security Event or Incident to the organization using applicable documents and any other resources.

iv) Determine what could be improved.

v) Communicate these findings to relevant stakeholders, as necessary, and for implementation of any recommendations made post-review of the Security Event or Incident.

vi) Carry out recommendations while ensuring that sufficient time and resources are committed to this activity.

5 Independence Way, Suite 300 201-577-4557 (o) EnrollmentxDesign.com
Princeton, NJ 08540 info@enrollmentxDesign.com

vii) Close the Security Event or Incident.

A. Retention and Review of Security Incident Record & Documentation

The process shall ensure investigation into the Security Incident and establish an incident record. The incident record should be verified during the follow up process to ensure that it documents:

1. All relevant factual information or evidence;

2. Consultations with stakeholders, partners, clients, and external advisors; and

3. Findings resulting from the collection of factual information or evidence obtained.

The rationale for the creation of an incident record is that law enforcement authorities may be informed of Security Incidents or ExD may take legal action if individuals causing a Security Incident can be identified. The implications of each Security Incident are not always discernible at the start of, or even during, the course of a Security Incident. Accordingly, it is important that information is documented and associated information system events are logged.

The incident record may be in written or electronic form. If it is maintained in an electronic form, appropriate protections must be applied to guard against the alteration or deletion of the incident record.

The information to be reported will vary according to the specific circumstances and availability of the information, but may include:

1. Dates and times when incident-related events occurred;

2. Dates and times when incident-related events were discovered;

3. Dates and times of incident-related conference calls;

4. A description of the Security Incident, including the systems, programs, networks or types of Information that may have been compromised;

5. Root cause(s) of the Security Incident(s), if known, and how they have been addressed;

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

6. An estimate of the amount of time spent by working to remediate incident-related tasks;

7. The amount of time spent by Third Parties working on incident-related tasks, including advice from outside counsel;

8. The names and contact information of all individuals providing information in connection with the investigation;

9. Measures taken to prevent future Security Incidents, taking into consideration root causes, along with any remediation costs incurred by ExD; and

10. If applicable, the date and time of law enforcement involvement.

All ExD partners and clients have an affirmative obligation to use reasonable efforts to respond to all inquiries for information and cooperate in all investigations.

Review of the incident record and documentation should include the following:

1. Review tracked documents of the Security Incident to evaluate the following:

- The causes of the nonconformity;
- Whether similar nonconformities exist or could potentially occur;
- The effectiveness of the corrective action taken; and
- The effectiveness of the Incident Response process.

2. Learn from Security Incidents and improve the response process. Security Incidents must be recorded and a post incident review conducted. Identify the impact of Security Incidents and outline pain points for future security investments. The following details must be retained:

- Types of Security Incidents
- Volumes of Security Incidents and malfunctions
- Costs incurred during the Security Incidents, where possible.

B. Periodic Evaluation of the Program

5 Independence Way, Suite 300
Princeton, NJ 08540
201-577-4557 (o)
info@enrollmentxDesign.com
EnrollmentxDesign.com

The processes surrounding incident response shall be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to Security Events and Incidents, as well as the training of the general population regarding the organization's expectation of them, relative to security responsibilities.

Security Events and Incidents shall be recorded for tracking, analysis, and reporting purposes. The following metrics should be considered to assess the overall Security Incident management program:

- Overall reduction in time spent responding to Security Incidents.
- Reduction of impact of certain Security Incidents.
- Overall reduction of the occurrence of Security Incidents.
- Mean time to analysis (MttA)
- Mean time to resolution (MttR)
